REMARKS

The present invention is a method of connecting user equipment to at least one network in a communication system comprising at least one network, including network entities which provide connectivity to the user equipment, a communication system comprising at least one network, including network entities which provide connectivity to user equipment and user equipment and a communications system comprising at least one network including network entities which provide connectivity to the user equipment. A method of connecting user equipment to the at least one network in a communication system comprising at least one network, including network entities which provide connectivity to the user equipment in accordance with an embodiment of the invention includes establishing a secure tunnel which provides connection between the user equipment and one of the network entities (Phase I) as illustrated in Figs. 7-18; and authenticating the user equipment with another of the network entities (Phase II) as illustrated in Figs. 7-18; and wherein the authentication of the user equipment with the another of the network entities occurs at least partially simultaneously with the establishing of the secure tunnel.

Claims 1-48 stand rejected under 35 U.S.C. §102 as being anticipated by U.S. Published Application 2002/0174335 (Zhang et al). The Examiner reasons as follows:

> Regarding claims 1-3, 6-8, 31-33, 35 and 40-42, Zhang discloses a method for providing authentication, authorization and accounting (AAA) transactions in a wireless network (see, for example, abstract and [0028]). Zhang discloses that a mobile terminal (MT) receives services from an Internet service provider (ISP) having an authentication server through an access point (AP) (corresponding to the recited access network) with a server (see, for example, Fig. 1 and [0073]). Zhang also discloses that a secure channel (i.e., secure

3

tunnel) is established between the MT and the AP (see, for example, [0025], [0026], [0043] and [0045]). Zhang further discloses that in one embodiment IPSEC is used for per-packet encryption between a MT and an AP (see, for example, [0029], [0067] and [0068]). In this embodiment every packet is encrypted and authenticated. As Fig. 2 and the procedure explained at [0073] through [0082] demonstrate that all transmitted messages are encrypted (corresponding to the recited establishing of the secure tunnel) while (corresponding to the recited at least partially simultaneous) authentication of a MT is being performed. This means that authentication process starts right after a secure channel is established.

These rejections are traversed for the following reasons.

Each of the independent claims 1, 31 and 40 substantively recites establishing a secure tunnel which provides connection between the user equipment and one of the network entities and authenticating the user equipment with another of the network entities which occurs at least partially simultaneously with the establishing of the secure tunnel. This subject matter has no counterpart in Zhang et al.

The Examiner reasons that Zhang's disclosure of the IPSEC protocol in establishing communications between the mobile terminal 110 and the access point 120 anticipates the subject matter of the claims. However, the Examiner has not considered the scope of the claims which require that the secure tunnel be established between the user equipment and one network entity and the authentication of the user equipment occurs with another network entity at least partially simultaneously with the establishing of the secure tunnel.

Even assuming arguendo that the Examiner's analysis of Zhang et al is otherwise correct, there is no counterpart of the claimed two different network entities which are involved with the establishment of the tunnel and the authenticating of the user equipment. This is readily apparent since there is only

4

one network entity 120 even involved with the process which the Examiner alleges anticipates. The IPSEC protocol is described as performing encryption between the mobile terminal 110 and only the wireless access point 120 which cannot anticipate the claimed <u>different</u> network entities which are involved with tunneling and authentication.

Moreover, the Examiner concludes "[t]his means that the authentication process starts right after a secure channel is established". This construction does not anticipate the independent claims for the reason that each of the independent claims requires the authenticating to occur at least partially simultaneously with the establishing of the secure tunnel. Therefore, assuming *arguendo* that the Examiner is correct in his assertion that the use of the IPSEC protocol involves the establishment of a secure tunnel, nevertheless the Examiner's construction thereof has established that the secure tunnel is established <u>before</u> the authentication process starts which does not anticipate the independent claims.

Moreover, IPSEC is understood to be a collection of security measures that comprise an optional tunneling protocol for IPV6. It is submitted that the Examiner has not established that the utilization of IPSEC to "insure data integrity as well as to prevent unauthorized users from pretending to be authorized ones" as stated in paragraph 67 of Zhang et al necessarily or inherently requires the establishment of a tunnel. It is submitted that the utilization of encryption does not, *per se*, establish that tunneling is utilized between the mobile terminal 110 and the wireless LAN 120. Accordingly, the independent claims are further not anticipated for the reason that there is no disclosure of tunneling being utilized as required by the claims.
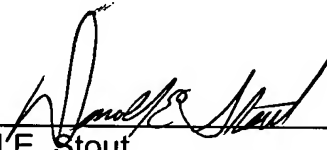
5

The dependent claims define further aspects of the present invention which are not anticipated by Zhang et al.

In view of the foregoing amendments and remarks, it is submitted that each of the claims in the application is in condition for allowance. Accordingly, early allowance thereof is respectfully requested.

To the extent necessary, Applicants petition for an extension of time under 37 C.F.R. §1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 01-2135 (0172.42240X00) and please credit any excess fees to such Deposit Account.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Donald E. Stout
Registration No. 26,422
(703) 312-6600

Attachments

DES:dlh

6